REMARKS

Claims 42-46, 48-54, 56, 58-62, and 64-66, 69, and 70-73 are pending. Claims 42, 50, and 58 are in independent form.

Objections to the Specification

In the action mailed February 1, 2008, the specification was objected to as failing to provide proper antecedent basis for a "second relying party," as recited in claims 48, 56, and 64. The objection cites to 37 C.F.R. § 1.75(d)(1) and M.P.E.P. § 608.01(o).

For the sake of convenience, 37 C.F.R. § 1.75(d)(1) is now reproduced.

> "(d)(1)The claim or claims must conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description." *See* 37 C.F.R. § 1.75(d)(1) (emphasis added).

As shown, the specification is not objectionable based solely on a failure to provide antecedent basis for the terms and phrases used in the claims. Instead, the specification can provide clear support for such terms and phrases and satisfy the requirements of 37 C.F.R. § 1.75(d)(1).

Applicant submits that clear support for a "second relying party" such as recited in claims 48, 56, and 64 is self-evident from the specification and its context. For example, the specification describes that a managed authentication service 8 can provide relying party 10 an out-sourced authentication service for verifying the identity of online visitors. *See, e.g., specification*, page 3, line 21-23. In particular, managed authentication service 8 allows relying party 10 to focus on providing its online service knowing that the authentication process is remotely handled by managed authentication service 8. *See, e.g., specification*, page 4, line 15-18. Relying party 10 is thus a customer of a managed authentication service 8 and accepts digital credentials managed by such a managed authentication service 8. *See, e.g., specification*, page 4, line 19-20.

The specification makes it clear that managed authentication service 8 is not limited to servicing a single customer, i.e., a single relying party 10. For example, in storing the result of a verification, managed authentication service 8 stores relevant transaction information that includes the identity of the relying party 10 that is involved in the transaction. *See, e.g., specification*, page 15, line 1-9. Applicant submits that such storing the identity of a relying

party 10 would be inappropriate were authentication service 8 limited to servicing a single customer, i.e., a single relying party 10.

As another example, the specification describes a plug-in 54 that initiates a challenge-response sequence that causes managed authentication service 8, or alternatively a relying party 10, to issue a challenge to the owner 4 of a digital signature. *See, e.g., specification*, page 16, line 22 - page 17, line 1. Such a challenge can include information that identifies relying party 10 so that the owner 4 can be assured that the message that he or she is signing can only be relied upon by that specific relying party. *See, e.g., specification*, page 17, line 5-9. Applicant submits that the need to identify a specific relying party bespeaks the ability of managed authentication service 8 to service multiple relying parties.

The specification thus supports the provision of an indication of a failure to authenticate digital credential information associated with a first user to a second relying party. Accordingly, the requirements of 37 C.F.R. § 1.75(d)(1) have been satisfied. Applicant requests that the objection to the specification be withdrawn.

Objections to the Claims

Claim 62 was objected to for reciting the "authentication server" rather than the "authentication service." Claim 62 has been amended to address the Examiner's concerns.

Rejections under 35 U.S.C. § 112

Claims 48, 56, and 64 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. The rejection contends that the specification does not reasonably convey to those skilled in the art that the inventors has possession of the provision of information indicative of a failure to authenticate the digital credential information associated with a first user to a second relying party, as recited in claims 48, 56, and 64.

Applicant respectfully disagrees. As discussed above, the specification makes it clear that that managed authentication service 8 is not limited to servicing a single customer, i.e., a single relying party 10. Instead, managed authentication service 8 performs various activities and takes certain precautions associated with the ability to service multiple customers, i.e., multiple relying parties.

Accordingly, the specification does reasonably convey to those skilled in the art that the inventors has possession of the provision of information indicative of a failure to authenticate the digital credential information associated with a first user to a second relying party, as recited in claims 48, 56, and 64. Applicant requests that the rejections of claims 48, 56, and 64 be withdrawn.

Rejections under 35 U.S.C. § 103

Claims 42, 50, and 58 were rejected under 35 U.S.C. § 103 as obvious over U.S. Patent No. 6,021,202 to Anderson et al. (hereinafter "Anderson"), U.S. Patent No. 6,275,941 to Saito et al. (hereinafter "Saito"), and U.S. Patent No. 6,047,270 to Joao et al. (hereinafter "Joao").

Claim 42 relates to a machine-implemented method that includes receiving digital credential information from a relying party at an authentication service, wherein the digital credential information is indicative of a first user being professionally licensed but has been received by the relying party from an unauthorized user, verifying that the digital credential information is valid using professional license status information that has been stored for a plurality of users, providing verification information indicative of a valid

professional license of the first user from the authentication service to the relying party, and providing information from the authentication service to the first user. The information is indicative of the provision of verification information indicative of the valid professional license to the relying party. The relying party, the unauthorized user, and the first user are distinct from each other.

Claim 50 relates to an article comprising a machine-readable medium embodying information indicative of instructions. When the instructions are performed by one or more machines of an authentication service, operations related to the method of claim 42 result.

Claim 58 relates to a system that includes an authentication service configured to perform activities related to the method of claim 42.

The rejections of claims 42, 50, and 58 contend that it would have been obvious for one of ordinary skill to have combined Anderson, Saito, and Joao to have arrived at the recited subject matter.

Applicant respectfully disagrees for several reasons. For example, the rejections contend that Anderson's FIG. 26 involves "digital credential information indicative of a first user being

professionally licensed" and that such digital credential information is allegedly verified as valid using professional license status information. *See id.*, page 4, line 9-18. ."

Applicant respectfully disagrees. Anderson's FIG. 26 depicts the use of a computer network in a medical record transaction. See, e.g., Anderson, col. 17, line 38-39. For the sake of convenience, Anderson's FIG. 26 and a written description thereof is now reproduced.

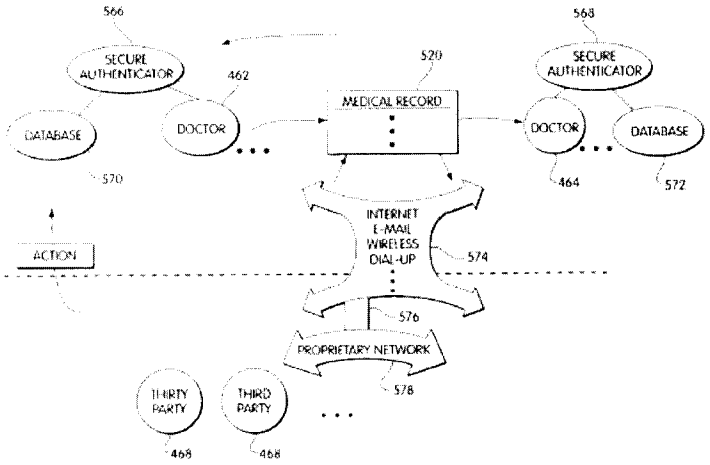

Fig. 26

"Referring to FIG. 26, the transmission of a medical record 520 is depicted wherein a first doctor 462 signs the medical record or a portion thereof 520 with the first doctor's secure authenticator 566 which permits a digital signature of the medical record 520. The signature may then be recorded in a database 570 which is responsive to the first doctor's secure authenticator. Once signed, the medical record 520 may be transmitted to a third party or to a second doctor 464. The second doctor may add material including a signature using the second doctor's secure authenticator 568. The second doctor's database 572 will record the signature

> and the additional information. Once signed by one or more doctors, the medical record 520 may be sent by a network 574 through a network connection 576 to a proprietary system 578 of one or more third parties 468, which could include an insurance company an administrative, or the like. Signatures, authentication, data manipulations, storage and retrieval, and other functions are accomplished in a manner similar to that used for the electronic check." *See id.*, col. 39, line 22-col. 40, line 11.

As discussed above, FIG. 26 describes the transmission of a medical record that is signed by one or more doctors. Such signatures are generally understood to identify the relevant doctor who signed the transmitted medical record, not the professional license status of the signing doctor. *See, e.g., id.*, col. 19, line 9-14 (describing that a FSML signature can be authenticated); col. 19, line 43-49 (describing that a medical record is an FSML electronic document that can be signed). Indeed, there is no verification of the professional license status of these doctors in this portion of Anderson.

This is perhaps not surprising given that Anderson's primary focus is on financial and other transactions that involve signed electronic documents. *See, e.g., Anderson*, col. 10, line 37-38. In particular, Anderson describes that a payer can electronically create a financial instrument that is payable to the order of the payee. *See, e.g., Anderson*, col. 23, line 41-44. The payer 12 signs and records the financial instrument

using a "secure authenticator" that enables the payer to digitally sign the financial instrument and enters the transaction in a secure log. *See, e.g., id.*, col. 23, line 41-49. The authenticator also appends cryptographically signed certificates of, e.g., the payer's bank and the federal reserve bank authenticating the payer's account and the payer's bank, to the financial instrument. *See, e.g., id.*, col. 23, line 50-54.

After receipt of the financial instrument, the payee validates the payer's digital signature using public key cryptography and verifies the payer's bank and the payer's account with the appended certificates. *See, e.g., id.*, col. 23, line 57-60. The transaction proceeds, and a Demand Deposit account is eventually issued to the payer to reflect the debit from the payer's account. *See, e.g., id.*, col. 24, line 38-42.

Like transmission of medical records discussed above, none of these processes have anything to do with professional license status information. However, Anderson does mention professional license status information. In particular, Anderson's Summary of the Invention describes that:

> "In one embodiment, the invention features a computer-based method in which an electronic instrument is created for effecting a transfer of funds from an account of a payer in a funds-holding institution to a payee, the instrument including an electronic signature of the payer. A digital representation of a verifiable certificate by the institution of the

> authenticity of the account, the payer, and the public key of the payer is appended to the instrument. This enables a party receiving the instrument, e.g., the payee or a bank, to verify the payer's signature on the instrument. A similar certificate of authenticity could also be issued in other contexts. For example, a certifying authority could certify that a doctor is properly licensed and authorized to sign a prescription." *See Anderson*, col. 11, line 13-26.

This is believed to be the only mention of professional license status in the entirety of Anderson's disclosure.

Despite the limited role that professional license status plays in Anderson's disclosure, the rejections contend that it would have been obvious for one of ordinary skill to have combined Anderson with various elements drawn from both Saito and Joao and to have arrived at the subject matter recited in claims 42, 50, and 58.

Applicant respectfully disagrees. First of all, even if one of ordinary skill were to fortuitously turn to the mention of professional license discussed above and combine it with both Saito and Joao, he or she would still not arrive at the subject matter recited in claims 42, 50, and 58.

In this regard, as discussed above, claims 42, 50, and 58 recite that valid digital credential information indicative of a first user being professionally licensed is received by a relying party from an unauthorized user, the validity of the

digital credential information is verified using professional license status information, and verification information indicative of a valid professional license of the first user is provided from the authentication service to the relying party. Further, information indicative of the provision of verification information indicative of the valid professional license to the relying party is provided to the first user. Thus, in claims 42, 50, and 58, information regarding the provision of verification information is provided to a first user notwithstanding the relying party having received the digital credential information indicative of the first user being professionally licensed from an unauthorized user.

Saito and Joao neither describe nor suggest that such information be provided. As discussed previously, Saito does not mention professional license status at all. Accordingly, there is no reason to believe that one of ordinary skill would find it obvious to provide information regarding the provision of such verification information indicative of a valid professional license of the first user, as recited in claims 42, 50, and 58.

As for Joao, Joao's focus is on preventing fraud in "credit card, charge card and/or debit card use, financial account, brokerage account, electronic money account, savings and/or

checking account activity and/or use and/or wireless or cellular communication device or telephone activity or use." *See, e.g., Joao*, col. 1, line 20-25. Please note that, despite the numerous contexts envisaged by Joao, fraud as to the validity of professional licenses is not among them.

Joao seeks to prevent fraud in these various contexts using systems that include point-of-sale devices (or, alternatively, "transaction devices"), a central processing computer, and any of a variety of "[cardholder] communication devices." *See, e.g., Joao*, FIGS. 1, 4, 7, 13. Upon receipt of data/information that is not associated with, e.g., a lost or stolen card, an overdrawn account, or the like, Joao's central processing computer asks the account holder to authorize the transaction via one of the communication devices. *See, e.g., Joao*, FIGS. 3A-3C, 6A-6C, 9A-9C, 12A-12C.

There are three circumstances envisaged by Joao that can occur after such a request to authorize, namely, the transaction is expressly authorized, the transaction is expressly not authorized, or there is no timely response to the request for authorization. *See, e.g., id.* Joao describes that the transaction could be consummated either when expressly authorized or, in the absence of a timely response, when circumstances warrant. *See, e.g., id.* Joao describes that the

transaction is not consummated either when not expressly authorized or, in the absence of a timely response, when circumstances warrant. *See, e.g., id.*

However, in no case does Joao describe that information regarding the provision of verification information is provided to a first user notwithstanding the relying party having received the digital credential information indicative of the first user being professionally licensed from an unauthorized user. Indeed, Joao's intended purpose is to prevent the provision of verification information to a relying party when the digital credential information is received from an unauthorized user. Since Joao allows transactions to be consummated, under certain circumstances, in the absence of a timely response, Joao does not completely foreclose the recited subject matter from occurring. However, Joao's intended purpose is to prevent unauthorized verifications and there is no reason to believe that those of ordinary skill would find the exceptions to Joao's intended purpose "obvious" in light of Anderson and Saito. Thus, even if Anderson, Saito, and Joao were combined, one of ordinary skill would not arrive at the recited subject matter. Accordingly, claims 42, 50, and 58 are not obvious over Anderson, Saito, and Joao on this basis.

Moreover, a rejection under 35 U.S.C. § 103(a) is proper only if the differences between the recited subject matter and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill. *See* 35 U.S.C. § 103(a). The subject matter as a whole encompasses not only the ability to modify the prior art, but also the desirability of the modification (*see, e.g., In re Fritch*, 972 F.2d 1260, 1266 n.14 (Fed. Cir. 1992), *citing In re Gordon*, 733 F.2d 900, 902, (Fed. Cir. 1984)) and the nature of the problem to be solved (*see, e.g., Pro-Mold & Tool Co. v. Great Lakes Plastics Inc.*, 75 F.3d 1568, 1573, (Fed. Cir. 1996), *citing In re Rinehart*, 531 F.2d 1048, 1054 (CCPA 1976)).

In the present case, there is a mention in passing of professional status information in one of the three references upon which the rejection is based. The present rejection takes this mention out of the context in which it is found and contends that handling professional status information in a manner that is neither described nor suggested by the cited references would have been obvious.

Indeed, there is no reason to believe that the need to inform a first user regarding the provision of verification information to a relying party notwithstanding the relying party having received the digital credential information indicative of

the first user being professionally licensed from an unauthorized user was recognized as desirable in any of the cited references. Indeed, Anderson only mentions professional license status in passing, while Saito and Joao do not mention it at all. Indeed, Joao intends to prevent unauthorized users of credit cards and other instruments from being able to use these instruments at all.

Accordingly, the rejection picks and chose unrelated teachings from the cited references and assembles them using applicant's own disclosure as a guide. Such hindsight-based reconstruction has never been recognized as acceptable in establishing obviousness. Accordingly, claims 42, 50, and 58 are not obvious over Anderson, Saito, and Joao on this basis, as well.

Applicant therefor requests that the rejections of claims 42, 50, 58, and the claims dependent therefrom be withdrawn.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally,

nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Applicant asks that all claims be allowed. Please apply the fee for a one month extension of time, along with any other charges or credits, to Deposit Account No. 06-1050.

Respectfully submitted,

Date: June 2, 2008

John F. Conroy
Reg. No. 45,485
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No. **20985**
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

JFC/jhg
10837345.doc